FINITE p-GROUPS OF CLASS 2 HAVE NONINNER AUTOMORPHISMS OF ORDER p

A. ABDOLLAHI

Dedicated to Professor Aliakbar Mohammadi Hassanabadi

ABSTRACT. We prove that for any prime number p, every finite non-abelian p-group G of class 2 has a noninner automorphism of order p leaving either the Frattini subgroup $\Phi(G)$ or $\Omega_1(Z(G))$ elementwise fixed.

1. **Introduction**

Let p be a prime number and G be a non-abelian finite p-group. A longstanding conjecture asserts that G admits a noninner automorphism of order p (see also Problem 4.13 of [7]). By a famous result of W. Gaschütz [3], noninner automorphisms of G of p-power order exist. M. Deaconescu and G. Silberberg [2] reduced the verification of the conjecture to the case in which $C_G(Z(\Phi(G))) = \Phi(G)$. H. Liebeck [5] has shown that finite p-groups of class 2 with $p > 2$ must have a noninner automorphism of order p fixing the Frattini subgroup elementwise. It follows from a cohomological result of P. Schmid [6] that the conjecture is true whenever G is regular. Here we show the validity of the conjecture when G is nilpotent of class 2. In fact we prove that

1991 *Mathematics Subject Classification.* 20D45;20E36.

Key words and phrases. Automorphisms of p-groups; nilpotent groups of class 2; noninner automorphisms.

This research was in part supported by a grant from IPM (No. 85200032).

Theorem. For any prime number p, every finite non-abelian p-group G of class 2 has a noninner automorphism of order p leaving either the Frattini subgroup $\Phi(G)$ or $\Omega_1(Z(G))$ elementwise fixed.

The unexplained notation is standard and follows that of Gorenstein [4].

2. **Preliminaries**

We use the following facts in the proof of the Theorem.

Remark 2.1. If G is a group whose derived subgroup G' is a finite cyclic p-group for some prime p, then $G' = \langle [a,b] \rangle$ for some $a, b \in G$. Since G' is generated by commutators $[x,y]$ $(x, y \in G)$ whose orders are p-powers and G' is abelian, $exp(G') = \max\{|[x,y]| \ : \ x, y \in G\}$. But G' is a finite cyclic group and so $exp(G') = |G'|$. Hence G' is generated by one of the elements of the set $\{[x,y] \ : \ x, y \in G\}$.

Remark 2.2. Let G be a finite nilpotent group of class 2 such that $G' = \langle [a,b] \rangle$ for some $a, b \in G$. Then by a well-know argument (e.g., see the proof of Lemma 1 of [1]) we have $G = \langle a, b \rangle \, C_G(\langle a, b \rangle)$. We give it here for the reader's convenience: for any $x \in G$, we have $[a,x] = [a,b]^s$ and $[b,x] = [a,b]^t$ for some integers s, t. Then $[a, b^{-s}a^t x] = 1$ and $[b, b^{-s}a^t x] = 1$. Hence $b^{-s}a^t x \in C_G(\langle a, b \rangle)$ and so $G = \langle a, b \rangle \, C_G(\langle a, b \rangle)$.

Remark 2.3. Let G be a nilpotent group of class 2, $x, y \in G$ and $k > 0$ be an integer. Then since $[y,x] = y^{-1}x^{-1}yx \in Z(G)$, it is easy to see by induction on k that $(xy)^k = x^k y^k [y,x]^{\frac{k(k-1)}{2}}$. Also we have $[x,y]^m = [x^m, y] = [x, y^m]$ for all integers m.

We shall make frequent use of Remark 2.3 without reference in the proof of the Theorem. Especially we use it in such a sample situation:

if we know that x and y are two elements in a nilpotent 2-group of class 2, $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $|[x, y]| = 2^n$ and $x^{m2^n} = y^{-2^n}$, then by Remark 2.3 and the hypothesis we have

$$(x^m y)^{2^n} = x^{m2^n} y^{2^n} [y, x^m]^{2^{n-1}(2^n-1)} = [y, x]^{m2^{n-1}(2^n-1)}.$$

Since $[x, y] = [x, x^m y]$ and $|[x, y]| = 2^n$, we have that $(x^m y)^{2^{n-1}} \neq 1$ and so $2^n \mid |x^m y|$. It follows that $|x^m y| = 2^{n+1}$, if m is odd, and $|x^m y| = 2^n$, if m is even.

Remark 2.4. Let G be a finite p-group of class 2. If G has no noninner automorphism of order p leaving $\Phi(G)$ elementwise fixed, then $Z(G)$ must be cyclic. In fact by the part (a) of the proof of [5, Theorem 1], we have G' is cyclic. Now if $Z(G)$ is not cyclic, then $\Omega_1(Z(G))$ is not cyclic and so $\Omega_1(Z(G)) \nleq G'$. Now take an element $z \in \Omega_1(Z(G)) \backslash G'$, a maximal subgroup M of G and $g \in G \backslash M$. Then the map α on G defined by $(mg^i)^\alpha = mg^i z^i$ for all $m \in M$ and integers i, is a noninner automorphism of order p leaving M (and so $\Phi(G)$) elementwise fixed, a contradiction.
Note that if $Z(G) = \Phi(G)$, then one may replace the latter argument by the part (iv) of Lemma 2 of [5].

Remark 2.5. Let G be a group and H, K be subgroups of G such that $G = HK$ and $[H, K] = 1$. If there exists a noninner automorphism φ of order p in $Aut(H)$ leaving $Z(H)$ elementwise fixed, then the map β on G defined by $(hk)^\beta = h^\varphi k$ for all $h \in H$ and $k \in K$ is a noninner automorphism of G of order p leaving $Z(G)$ elementwise fixed. It is enough to show that β is well-defined and this can be easily seen, because $x^\varphi = x$ for all $x \in H \cap K = Z(H)$, by hypothesis.

3. **Proof of the Theorem**

By the main results of [2] and [5], we may assume that $\Phi(G) = C_G(Z(\Phi(G)))$ and $p = 2$. By Remark 2.4, we may further assume that $Z(G)$ is cyclic. Now Remark 2.1 implies that there exist elements $a, b \in G$ such that $G' = \langle [a,b] \rangle$. Let $H = \langle a, b \rangle$. Then it follows from Remark 2.2 that $G = HC_G(H)$ and by Remark 2.5 it is enough to construct a noninner automorphism φ of H of order 2 leaving $Z(H)$ elementwise fixed.

Note that $|G'| = |H'| = |[a,b]| = 2^n$ for some integer $n > 0$. Since G' is cyclic and $G' \leq Z(G)$,

$$\exp(\frac{G}{Z(G)}) = \exp(\frac{H}{Z(H)}) = 2^n,$$

which implies that $Z(H) = \left\langle a^{2^n}, b^{2^n}, [a,b] \right\rangle \leq Z(G)$. If $n = 1$, then $\Phi(G) = G^2 \leq Z(G)$. Since $\Phi(G) = C_G(Z(\Phi(G)))$, we have $G = \Phi(G)$, which is impossible. Therefore $n \geq 2$. Since $Z(H)$ is cyclic, either $a^{2^n i} = b^{2^n}$ or $a^{2^n} = b^{2^n i}$ for some integer i. Suppose that $a^{2^n i} = b^{2^n}$. If i is even, then $|a^{-i}b| = 2^n$ and $(a^{-i}b)^{2^{n-1}} \notin Z(H)$, as $[a,b] = [a, a^{-i}b]$ has order 2^n. If $c = a^{-i}b$, then the map φ on H defined by $(a^s c^t x)^\varphi = (ac^{2^{n-1}})^s c^t x$ for all $x \in Z(H)$ and integers s, t, is a noninner automorphism of H of order 2 leaving $Z(H)$ elementwise fixed. If $a^{2^n} = b^{2^n i}$ and i is even, then we can similarly construct such a $\varphi \in Aut(H)$. Hence, from now on we may assume that $a^{2^n i} = b^{2^n}$ for some odd integer i and so $c = a^{-i}b$ has order 2^{n+1}.

Now suppose that $[a,b] \in \left\langle a^{2^n} \right\rangle$. Then $Z(H) = \left\langle a^{2^n} \right\rangle$ and so $|a^{2^n}| \geq 2^n$. Thus $a^{2^n j} = c^{2^n}$ for some integer j. Since $n \geq 2$, $|a^{2^n}| \geq 2^n$ and $|c| = 2^{n+1}$, j must be even. This implies that $d = a^{-j}c$ has order 2^n and $d^{2^{n-1}} \notin Z(H)$, as $[a,b] = [a,d]$ is of order 2^n. Hence the map φ on G defined by $(a^s d^t x)^\varphi = (ad^{2^{n-1}})^s d^t x$ for all $x \in Z(H)$ and integers s, t

is the desired automorphism φ of H.

Thus we may assume that $[a,b] \notin \left\langle a^{2^n} \right\rangle$. Since $Z(H) = \left\langle a^{2^n}, [a,b] \right\rangle$ is cyclic, it follows that $Z(H) = \langle [a,b] \rangle = H'$. On the other hand

$$\frac{H}{Z(H)} = \langle aZ(H) \rangle \times \langle bZ(H) \rangle$$

and $|\langle aZ(H) \rangle| = |\langle bZ(H) \rangle| = 2^n$, which implies that the element $e = a^{-2^{n-1}i} b^{2^{n-1}}$ does not belong to $Z(H)$ and $|e| = 2$ as $n \geq 2$. Now the map φ on H defined by $(a^s b^t x)^\varphi = (ae)^s (be)^t x$ for all $x \in Z(H)$ and integers s,t is the required automorphism φ. This completes the proof. $\square$

Acknowledgement. The author thanks the Center of Excellence for Mathematics, University of Isfahan.

References

[1] J.E. Adney and Ti Yen, *Automorphisms of a p-group*, Illinois J. Math. **9** (1965) 137-143.

[2] M. Deaconescu, G. Silberberg, *Noninner automorphisms of order p of finite p-groups*, J. Algebra **250** (2002) 283-287.

[3] W. Gaschütz, *Nichtabelsche p-Gruppen besitzen äussere p-automorphismen*, J. Algebra **4** (1966) 1-2.

[4] D. Gorenstein, *Finite Groups*, Harper & Row, New York, 1968.

[5] H. Liebeck, *Outer automorphisms in nilpotent p-groups of class 2*, J. London Math. Soc. **40** (1965) 268-275.

[6] P. Schmid, *A cohomological property of regular p-groups*, Math. Z. **175** (1980) 1-3.

[7] Unsolved problems in group theory, The Kourovka Notebook, No. 16, Edited by V. D. Mazurov and E. I. Khukhro, Russian Academy of Sciences, Siberian Division, Institue of Mathematics, Novosibirisk, 2006.

Department of Mathematics, University of Isfahan, Isfahan 81746-73441, Iran; and Institute for Studies in Theoretical Physics and Mathematics (IPM).

E-mail address: a.abdollahi@math.ui.ac.ir